

(19)



JAPANESE PATENT OFFICE

## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **06068117 A**(43) Date of publication of application: **11.03.94**

(51) Int. Cl

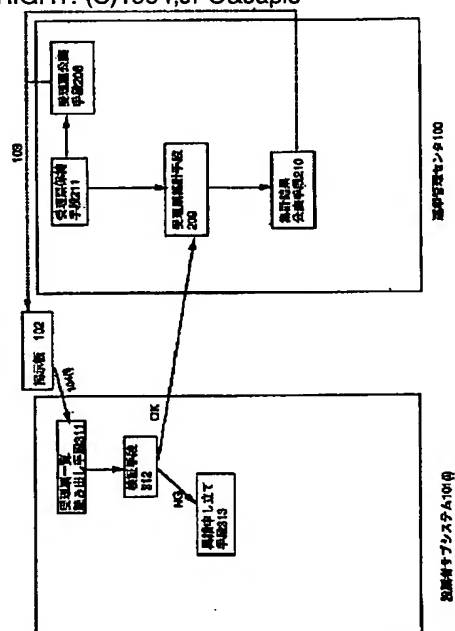
**G06F 15/28**(21) Application number: **04222580**(71) Applicant: **NEC CORP**(22) Date of filing: **21.08.92**(72) Inventor: **SAKO KAZUE**(54) **ELECTRONIC VOTING DEVICE**

COPYRIGHT: (C)1994,JPO&amp;Japio

## (57) Abstract:

**PURPOSE:** To raise an objection to a case when present vote is not accepted for the vote collection while it is not known to other voters to whom the voter has voted by making all voting slips received by an election manager in public while being ciphered.

**CONSTITUTION:** A voter 101(i) reads a content written on a bulletin board 102 and uses a voting paper generating means to generate a voting slip composed of an approval slip, an objection slip and a voting tag along with a read format. The received slip publication means 208 of a center 100 makes all received slips and the list of tags in public. Each voter 101(i) uses a received slip list read means 311 to reads the slit of the accepted slips and the voting tags, and uses a verification means 312 to confirm that its voting is included in the list of the accepted slips and the voting tags. When not confirmed, the voter uses an objection means 313 to raise an objection. When no objection is received, a decoding key is used to decode all the accepted slips.



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平6-68117

(43)公開日 平成6年(1994)3月11日

(51)Int.Cl.<sup>5</sup>

G 0 6 F 15/28

識別記号

庁内整理番号

F I

技術表示箇所

B 7052-5L

審査請求 有 請求項の数3(全 13 頁)

(21)出願番号 特願平4-222580

(22)出願日 平成4年(1992)8月21日

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 佐古 和恵

東京都港区芝五丁目7番1号日本電気株式会社内

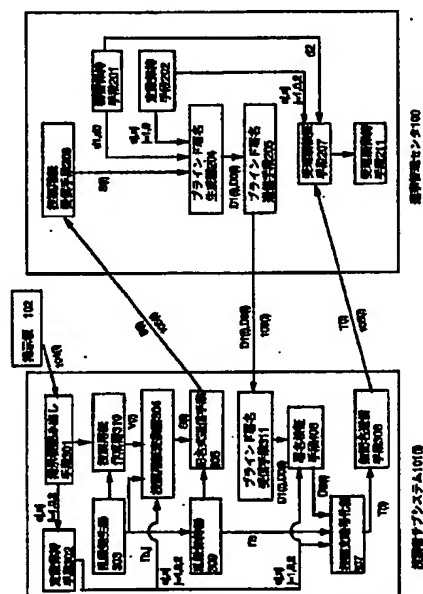
(74)代理人 弁理士 京本 直樹 (外2名)

(54)【発明の名称】 電子投票装置

(57)【要約】

【目的】 本発明では、投票者が自分が何に投票したかを他の投票者に知られることなく不正集計に対して異議申し立てをオープンにできる方式において、同一投票者が2つ以上の選択肢に投票することを検出でき、かつこの検出機構を第三者に悪用されない方式を提案することを目的とする。

【構成】 選択肢毎の投票用紙を、公開鍵暗号の秘密鍵で署名し、署名された投票用紙と、対応する公開鍵暗号の検証鍵（投票タグと呼ぶ）に対して選挙管理者のブラインド署名を得る投票用紙設定手段と、ブラインド署名で得た署名と投票者がつけた署名の両方をもつ投票用紙と投票タグの対を暗号化して無記名で選挙管理者に送付する投票手段と、選挙管理者は受理したすべての投票文を暗号化されたまま公開する票公開手段と、自分の投票が受理されていない異議申し立てを行なう票確認手段からなる。



## 【特許請求の範囲】

【請求項1】 投票者が投票用紙を変換して送出する投票用紙変換手段と、

選挙管理者が正当な有権者の投票用紙に対して署名をし、それを投票者に返信する署名手段と、  
各投票者が返信された署名文を用いて投票文に対する署名文を作成し、投票内容を暗号化して無記名で送付する投票手段と、

選挙管理者が受け取ったすべての投票文を暗号化されたまま公開する票公開手段と、

投票者が自分の投票が受理されていなければ異議申し立てを行なう受理票確認手段と、

異議申し立てがなければ、すべての票を復号化して正当な署名文が付加された投票文を集計し、公表する集計手段を有することを特徴とする電子投票装置。

【請求項2】 投票者が投票用紙を変換して送出する投票用紙変換手段と、

選挙管理者が正当な有権者の投票用紙に対して署名をし、それを投票者に返信する署名手段と、

各投票者が返信された署名文を用いて投票文に対する署名文を作成し、署名付きの投票文を無記名で送付する投票手段と、

選挙管理者が受け取ったすべての投票文を暗号化して公開する票公開手段と、

投票者が自分の投票が受理されていなければ異議申し立てを行なう受理票確認手段と、

異議申し立てがなければ、すべての票を復号化して正当な署名文が付加された投票文を集計し、公表する集計手段を有することを特徴とする電子投票装置。

【請求項3】 投票者が投票用紙を変換して送出する投票用紙変換手段と、

選挙管理者が正当な投票者の投票用紙に対して署名をし、それを投票者に返信する署名手段と、

各投票者が返信された署名文を用いて投票文に対する署名文を作成し、署名付きの投票文を無記名で送付する投票手段、

及び正当な署名文が付加された投票文を集計し、公表する集計手段を有する電子投票装置において、投票用紙として、各選択肢に対応する署名付き投票内容と検証鍵を含み、投票文として選択肢と検証鍵を含むことを特徴とする電子投票装置。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 本発明は電子ネットワーク上で有権者だけが1度だけ無記名で投票でき、投票者が自分が何に投票したかを他の投票者に知られることなく、自分の票が集計用に受理されなかった場合に異議申し立てを行なうことができる電子投票装置に関する。

## 【0002】

【従来の技術】 電子投票方法として従来から知られてい

るものは太田の方法がある。これは特開平1-177164号及び昭和63年電子情報通信学会春季全国大会A-294「単一の選挙管理者を用いた電子投票方式」に開示されている。この方式は投票者は乱数で変換した投票内容に対してセンタの署名を得た後、投票者側で乱数成分を取り除いたもとの投票内容に対するセンタの署名を作成し、これを無記名でセンタに送ることにより無記名投票を実現している。各投票者は自分の投票が受理・集計されたことを、センタが発表する投票内容一覧で確認する。この方法では自分の意見を反映させた投票内容に対してのみセンタの署名を得られるので、センタがその投票内容を集計しなかった場合、自分の投票内容を公開して異議申し立てを行わなくてはならない。

【0003】 この問題を解決すべく、異議申し立てを行なう場合も、投票者が自分の投票内容を公開せずに異議申し立てを行なうために、あらかじめ投票内容に依存しない投票用紙にのみ署名をもらい、署名付きの投票用紙に自分の意見を反映させた投票内容をセンタに送るという方式が、特願平4-108069号で示された。実施例として、各有権者は賛成票・反対票及び投票タグからなる署名つき投票用紙を記名式で入手し、そのうち一方の票を投票タグと共に無記名で投票する方式が述べられている。

## 【0004】

【発明が解決しようとする課題】 特願平4-108069号や太田の方式において、異議申し立ては集計結果判明後に行なう。したがって、賛成・反対の2値の投票を行なう場合、異議申し立て者は集計結果と反対の票に投じたと類推されるという問題点がある。本発明ではこのような投票を無効にする電子投票装置を提案する。

【0005】 また、特願平4-108069号においては、投票タグに対応する賛成票・反対票を選挙管理センタが容易に偽造できるので、下記の問題が発生する。たとえば投票者Aが賛成票 $v_1$ 、反対票 $v_0$ と投票タグ $v_t$ の署名を得、賛成票 $v_1$ と投票タグ $v_t$ を匿名で送付したとする。このとき、センタが反対票 $v'_0$ を偽造して、これとタグ $v_t$ を受理したと発表したとする。投票者の異議申し立て時には、投票者は $v_1$ 、 $v_0$ 、 $v_t$ を公開しセンタの不正を暴くことができるが、同時に自分が賛成票に投じたことも他の投票者にわかってしまうという問題点がある。なぜならば $v_t$ をタグとして用いた反対票に対して異議申し立てをしているからである。本発明ではこの問題点も解決する電子投票装置を提案する。

## 【0006】

【課題を解決するための手段】 第一の発明の電子投票装置は、投票者が投票用紙を変換して送出する投票用紙変換手段と、選挙管理者が正当な有権者の投票用紙に対して署名をし、それを投票者に返信する署名手段と、各投票者が返信された署名文を用いて投票文に対する署名文

10

20

30

40

50

を作成し、投票内容を暗号化して無記名で送付する投票手段と、選挙管理者が受け取ったすべての投票文を暗号化されたまま公開する票公開手段と、投票者が自分の投票が受理されていないければ異議申し立てを行なう受理票確認手段と、異議申し立てがなければ、すべての票を復号化して正当な署名文が付加された投票文を集計し、公表する集計手段を有することを特徴とする。

【0007】第二の発明の電子投票装置は、投票者が投票用紙を変換して送出する投票用紙変換手段と、選挙管理者が正当な権者の投票用紙に対して署名をし、それを投票者に返信する署名手段と、各投票者が返信された署名文を用いて投票文に対する署名文を作成し、署名付きの投票文を無記名で送付する投票手段と、選挙管理者が受け取ったすべての投票文を暗号化して公開する票公開手段と、投票者が自分の投票が受理されていないければ異議申し立てを行なう受理票確認手段と、異議申し立てがなければ、すべての票を復号化して正当な署名文が付加された投票文を集計し、公表する集計手段を有することを特徴とする。

【0008】第三の発明の電子投票装置は、投票者が投票用紙を変換して送出する投票用紙変換手段と、選挙管理者が正当な投票者の投票用紙に対して署名をし、それを投票者に返信する署名手段と、各投票者が返信された署名文を用いて投票文に対する署名文を作成し、署名付きの投票文を無記名で送付する投票手段、及び正当な署名文が付加された投票文を集計し、公表する集計手段を有する電子投票装置において、投票用紙として、各選択肢に対応する署名付き投票内容と検証鍵を含み、投票文として選択肢と検証鍵を含むことを特徴とする。

【0009】

【実施例】 つぎに、図1から図8を参照して第一、第二および第三の発明の実施例について説明する。

【0010】本発明の電子投票装置を、図3のように、 $m$ 個の投票者サブシステム101(1)～101( $m$ )及び1つの選挙管理センタ100が相互に安全な通信チャネル(例えばデータ回線)105で結ばれており、さらに選挙管理センタ100のみが書き込み可能な掲示板で、すべての投票者サブシステムが読み出せる電子掲示板102が存在する場合の無記名電子投票システムに実施する例を述べる。なお、以下簡単のために選挙管理センタをセンタ、投票者サブシステムを投票者と呼ぶことにする。

【0011】また、本実施例では簡単のために投票内容は賛成あるいは反対の2値とするが、多値にも容易に拡張できる。

【0012】この投票システムは準備フェーズと、投票用紙設定フェーズ、投票フェーズおよび結果公表フェーズからなる。

【0013】第一及び第二の発明は投票フェーズ及び結果公表フェーズに関する。

【0014】まず、図1, 2, 4を用いて第1の発明の準備フェーズを説明する。

【0015】本無記名電子投票システムを実施するための準備として、センタ100は署名用の定数を設定し、検証用定数を電子掲示板102に掲示する。例えば、署名方式としてRSA暗号方式を用いるとする。そこで、 $n_1, n_0, n_2$ を各々二つの素数 $p_1, q_1$ 及び $p_0, q_0$ 並びに $p_2, q_2$ の積とし、 $e_1, e_0, e_2$ と $d_0, d_1, d_2$ を $e_i \cdot d_i = 1 \bmod (p_i - 1)(q_i - 1)$  ( $i=1, 0, 2$ )を満たす整数とする。このときセンタは $e_i, n_i$  ( $i=1, 0, 2$ )を検証用定数として設定する(ステップ11)。これらの定数を電子掲示板102に書き込む(ステップ12)。今後この検証用定数 $e_i, n_i$  ( $i=1, 0, 2$ )は頻繁に用いられるので自分の定数保持手段201に書き込み容易にアクセスできるようにする(ステップ13)。一方、 $d_1, d_0, d_2$ は自分の秘密情報保持手段202に格納する(ステップ14)。

【0016】次に、センタ100は投票に関する規則を定める。まず、投票対象の議題を明らかにし、1組の賛成票・反対票及びタグ票の投票フォーマットを定める。たとえば、以下のような投票フォーマットを考える。ステップ11で設定された $n_j$  ( $j=1, 0, 2$ )がそれぞれ512ビットであり、 $n_1 < n_2$ とする。上位第1ビットから第8ビットの排他的論理和が1のとき賛成、0のとき反対とする。次に第9ビットから、第249ビットには任意の整数が入れ、次の192ビットは、第1ビットから第56ビットをDES暗号の鍵、第57ビットから第249ビットを平文とみなした場合の暗号文とするフォーマットとする。このように設定した512ビットの数字が $n_1$ より小さくなるようにする。また、タグ票は上位第1ビットから第8ビットをすべて0にし、第9ビットから、第249ビットには任意の整数が入れ、次の192ビットは、第1ビットから第56ビットをDES暗号の鍵、第57ビットから第249ビットを平文とみなした場合の暗号文とするフォーマットとする。このように設定した512ビットの数字が $n_0$ より小さくなるようにする(ステップ15)。

【0017】次に、投票する権利のあるサブシステム(以後、有権者と呼ぶ)の名前を一覧にする(ステップ16)。投票用紙作成及び投票の期限を設定・公表し(ステップ17)、投票用紙作成フェーズの開始を合図する(ステップ18)。

【0018】以上が準備フェーズである。

【0019】次に、投票用紙作成フェーズ、及び投票フェーズを説明するが、両フェーズとも選挙管理センタ100は各投票者に対して同じ手順を踏むので、特定の投票者サブシステム101( $i$ )に対する手順を例にとりて説明を続ける。

【0020】図1に示すように無記名電子投票システム

はセンタ100が電子掲示板102に定数及び投票規則を書き込む安全通信チャネル103、投票者101

(i)が電子掲示板102に書かれた内容を読み出すための安全通信チャネル104(i)および投票者とセンタが交信するための安全通信チャネル105(i)で構成されている。

【0021】まず、図1を参照しながら投票者101

(i)の投票用紙作成フェーズを説明する。

【0022】投票者101(i)は掲示板読み出し手段301を用いて掲示板102に書かれてある内容を読み出し、定数 $e_j$ ,  $n_j$  ( $j=1, 0, 2$ )を定数保持手段302に格納する一方、読み出したフォーマットに沿うよう投票用紙作成手段310にて賛成票 $v_1, 1$ ・反対票 $v_1, 0$ ・投票タグ $v_0, 0$ からなる投票用紙V

(i)を生成する。これを

$V(i) = (v_1, 1, v_1, 0, v_0, 0)$

と表す。なお、各賛成票・反対票及び投票タグ作成にあたってフォーマットに必要な乱数成分は乱数発生器303の出力を用いる。

【0023】次に、投票用紙変換器304は、乱数発生器303の出力 $r_b, j$ と定数 $e_b, n_b$  ( $b=1, 0$ )を用いて、

【0024】

【数1】

$$S_{b,j} = v_{b,j} \cdot r_b^{n_b} \cdot \text{mod } n_b$$

【0025】を $(b, j) = (1, 0), (1, 1), (0, 0)$ のそれぞれに対して計算し、 $s_{b,j}$ からなるベクトル $S(i) = (s_1, 1, s_1, 0, s_0, 0)$ を出力する。また、このときの乱数発生器303の出力 $r_b, j$ は乱数保持器309に格納する。S

(i)を記名付き交信手段305が安全チャネル105\*

$$t_{1,B} = ((d_{1,B} / r_1, B) \text{ mod } n_1) e_2 \text{ mod } n_2$$

$$t_{0,0} = d_{0,0} / r_{0,0} \text{ mod } n_0$$

を計算し、無記名送信手段308は $T(i) = (t_{1,B}, t_{0,0})$ を送信者名を付記せずにセンタ100に送出する。

【0035】センタ100は、受信した $T(i)$ のうち $t_{0,0}$ を読み出し

【0036】

【数4】

$$\alpha = t_{0,0}^{n_0} \text{ mod } n_0$$

【0037】を計算する。 $\alpha$ は投票者が不正をしていなければ、 $v_{0,0}$ に等しくなる。 $\alpha$ があらかじめ定められたタグのフォーマットであれば、これと同じタグが以前使われているかどうか検証する。使われていなければ、 $t_{1,B}$ を受理票とするとともに、使用済タグとして $\alpha$ を記録する。 $t_{1,B}, \alpha$ を受理票保持手段211に格納する。同じタグが使われていれば、無効票として受理しない。

【0038】以上が投票フェーズである。全員の投票が

\* (i)を通じてセンタ100に送信する。

【0026】センタ100は投票用紙受信手段206で受信した正当な有権者からの $S(i)$ を受信する。ブラインド署名生成器204は秘密保持手段201、定数保持手段202から読みだした $d_b$ 及び $n_b$ を用いて、

【0027】

【数2】

$$D_{b,j} = s_{b,j}^{n_b} \text{ mod } n_b$$

【0028】を各 $(b, j) = (1, 0), (1, 1), (0, 0)$ について計算し、出力する。ブラインド署名送信手段205は $D(i) = (D_1, 0, D_1, 1, D_0, 0)$ を投票者101(i)に送信する。

【0029】投票用紙作成を行なったすべての有権者に対して署名を送信すればセンタは投票フェーズに移行することを宣言する。以上が投票用紙設定フェーズである。

【0030】次に、投票フェーズを説明する。

【0031】署名検証手段306は、ブラインド署名受信手段311によりセンタ100から受信した $D(i)$ と、定数保持手段302から読み出した $e_b, n_b$ を用いて

【0032】

【数3】

$$s_{b,j} = d_{b,j}^{n_b} \text{ mod } n_b$$

【0033】が各 $(b, j) = (1, 0), (1, 1), (0, 0)$ について成立するかどうか検証する。

【0034】確認できれば、投票暗号化器307は、自分の意見 $B$  ( $B$ は0か1)に対して、乱数保持器309から読み出した整数 $r_1, B, r_0, 0$ と、定数保持手段302から読み出した $n_1, n_0, e_2$ を用いて、

終了したら、センタは結果公表フェーズへ移る。

【0039】次に図2を用いて結果公表フェーズを説明する。

【0040】センタ100は受理票公表手段208において、受け取ったすべての受理票とそのタグの一覧を公表する。各投票者101(i)は受理票一覧読み出し手段311において、受理票と投票タグの一覧を読み出し、検証手段312において自分の投票が票及びタグが一覧に含まれていることを確認する。確認できなければ、異議申し立て手段313を用いて異議申し立てを行なう。これについては後で詳細に述べる。センタはどの投票者からも異議申し立てがなければ、復号鍵 $d_2$ を用いてすべての受理票を復号化し、 $e_1$ を用いて署名を確かめる。すなわち、

【0041】

【数5】

$$\beta = (t_{1,B}^{n_1} \text{ mod } n_2)^{e_1} \text{ mod } n_1$$

【0042】が定められたフォーマットに従った正当な票になっていることを確かめる。確かめられればこの票の値に基づいて集計を行なう。確かめられない場合は無効票とする。

【0043】全部の票が集計できれば、復号鍵とともに集計結果を公表する。各投票者は受理票を復号鍵で復号すれば公表された集計結果になることを検証できる。

【0044】一方、検証手段312において自分の投票が受理されていないければ、異議申し立て手段313において、以下をとり行なう。

【0045】ブラインド署名受信手段311にて受信し、署名検証手段306において検証された $D(i)$ と、定数保持手段302から読み出した $e_b, n_b$ をおよび乱数保持手段309から読み出した $r_b, j$ を用いて $r_{b,j} = s_{b,j} / r_{b,j} \bmod n_b$ 各 $(b, j) = (1, 0), (1, 1), (0, 0)$ について計算し、異議申し立て時に公表する。

【0046】

【数6】

$$r_{b,j} \bmod n_b$$

【0047】となる $j = 0, 1$ のいずれもの受理票および

$r_0, 0$

のタグが公表されていないことが確認されれば、異議申し立て者の票が受理されていないと処理される。

【0048】このように異議を申し立てれば、異議申し立て者が実際はどちらの票を投票したのかを明らかにすることなく、自分の票が受理されなかったことを証明することができる。さらに、異議申し立て時には全体の投票結果は暗号化されたままなので、投票結果に対する異議とは区別され、従来の方式の様に異議申し立て者が投票結果が不満で異議を唱えているのではないことが明らかになる。

【0049】なお、本発明を賛成・反対両方に投票する不正投票者が存在しない場合に適用する場合には、投票タグは一切用いなくても同じ効果をもたらす。

【0050】次に図6、7を用いて第二の発明の実施例を説明する。

【0051】第二の発明は、第一の発明と同様、集計結果を公開する前に、暗号化された受理票を公開して、自分の投票が集計されているかどうかを見るにする。第一の発明では投票者が自分の投票内容をセンタの公開鍵で暗号していたが、第二の発明では処理能力の大きいセンタが、受理した投票を公開鍵で暗号化して公表することにする。これにより、投票者の負担軽減が見込まれる。

【0052】上記の第一の発明の実施例と準備フェーズ、投票用紙作成フェーズは同様であるが、投票フェーズにおける投票文作成器500と公表フェーズにおける受理票暗号化手段501が異なっているので差異だけ説明する。投票文作成器500では自分の意見 $B$  ( $B$ は0

か1)に対して、乱数保持器309から読み出した整数 $r_1, B, r_0, 0$ と、定数保持手段302から読み出した $n_1, n_0$ を用いて、

$$t_1, B = (d_1, B / r_1, B) \bmod n_1$$

$$t_0, 0 = d_0, 0 / r_0, 0 \bmod n_0$$

を計算し、無記名送信手段308は $T(i) = (t_1, B, t_0, 0)$ を送信者名を付記せずにセンタ100に送出する。

【0053】センタは受理票検証手段207でこれの正当性を検証できれば受理票保持手段211に格納する。

【0054】以上が投票フェーズである。

【0055】公表フェーズにおいては、センタは受理票保持手段211に格納されている受理票をあらかじめ公開してある公開鍵 $e_2, n_2$ を用いて暗号化し、暗号化された受理票を公表する。各投票者の検証手段312では、自分の票を公開鍵 $e_2, n_2$ で暗号化したものと比較して、自分の票が受理されているか否かを調べる。

【0056】次に図4、8を用いて第三の発明の実施例を説明する。第三の発明は主に投票用紙設定フェーズに関する。

【0057】まず、図4を持ちいて第三の発明の準備フェーズを説明する。

【0058】本無記名電子投票システムを実施するための準備として、センタ100は署名用の定数を設定し、検証用定数を電子掲示板102に掲示する。例えば、署名方式としてRSA暗号方式を用いるとする。そこで、 $n_1, n_0, n_2$ を各々二つの素数 $p_1, p_1$ 及び $p_0, p_0$ 並びに $p_2, p_2$ の積とし、 $e_1, e_0, e_2$ と $d_1, d_0, d_2$ を $e_i \cdot d_i = 1 \bmod (p_i - 1)(q_i - 1)$  ( $i = 1, 0, 2$ )を満たす整数とする。このときセンタは $e_i, n_i$  ( $i = 1, 0, 2$ )を検証用定数として設定する(ステップ11)。これらの定数を電子掲示板102に書き込む(ステップ12)。今後この検証用定数 $e_i, n_i$  ( $i = 1, 0, 2$ )は頻繁に用いられるので自分の定数保持手段621に書き込み容易にアクセスできるようにする(ステップ13)。一方、 $d_1, d_0, d_2$ は自分の秘密情報保持手段622に格納する(ステップ14)。

【0059】次に、センタ100は投票に関する規則を定める。まず、投票対象の議題を明らかにし、1組の賛成票・反対票及びタグ票の投票フォーマットを定める。たとえば、以下のような投票フォーマットを考える。ステップ11で設定された $n_1$ が512ビットであり、上位第1ビットから第8ビットの排他的論理和が1のとき賛成、0のとき反対とする。次に第9ビットから、第249ビットには任意の整数が入れ、次の192ビットは、第1ビットから第56ビットをDES暗号の鍵、第57ビットから第249ビットを平文とみなした場合の暗号文とするフォーマットとする。このように設定した512ビットの数字が $n_1$ より小さくなるようにする

(ステップ15)。

【0060】次に、投票する権利のあるサブシステム（以後、有権者と呼ぶ）の名前を一覧にする（ステップ16）。投票用紙作成及び投票の期限を設定・公表し（ステップ17）、投票用紙作成フェーズの開始を合図する（ステップ18）。

【0061】以上が準備フェーズである。

【0062】次に、投票用紙作成フェーズ、及び投票フェーズを説明するが、両フェーズとも選挙管理センタ100は各投票者に対して同じ手順を踏むので、特定の投票者サブシステム101(i)に対する手順を例にとつて説明を続ける。

【0063】図6に示すように無記名電子投票システムはセンタ100が電子掲示板102に定数及び投票規則を書き込む安全通信チャネル103、投票者101

(i)が電子掲示板102に書かれた内容を読み出すための安全通信チャネル104(i)および投票者とセンタが交信するための安全通信チャネル105(i)で構成されている。

【0064】図6を参照しながら投票者101(i)の投票用紙作成フェーズを説明する。

【0065】投票者101(i)は掲示板読み出し手段601を用いて掲示板102に書かれてある内容を読み出し、定数 $e_j$ ,  $n_j$  ( $j=1, 0, 2$ )を定数保持手段602に格納する。

【0066】次に投票用紙作成手段610にて以下を行なう。乱数発生器603の出力を用いて署名用の定数を設定する。ここではRSA署名を用いるとし、署名鍵 $d$ 、検証鍵 $e$ ,  $n$ を定める。ここで、 $n$ は $n_1$ より小さく、 $e$ ,  $n$ を連結したものが $n_0$ より小さくなるようにする。たとえば $n$ を520ビット、 $e$ を10ビット、 $n_0$ は530ビットなどと準備フェーズでセンタがあらかじめ決めておけばよい。

【0067】次にフォーマットに沿った $n$ より小さい賛成票 $u_{1,1}$ ・反対票 $u_{1,0}$ を定め、それらの署名文

【0068】

【数7】

$$v_{b,j} = \overline{v_{b,j}} \cdot r_{b,j}^e \cdot \text{mod } n \quad (b=1, 0)$$

【0069】を求める。投票タグ $u_{0,0}$ は $e$ ,  $n$ を連結したものとす。この3組を投票用紙 $V(i)$ とし、 $V(i) = (v_{1,1}, v_{1,0}, v_{0,0})$ と表す。次に、投票用紙変換器604は、乱数発生器603の出力 $r_{b,j}$ と定数 $e_b$ ,  $n_b$  ( $b=1, 0$ )を用いて、

【0070】

【数8】

$$s_{b,j} = v_{b,j} \cdot r_{b,j}^e \cdot \text{mod } n.$$

【0071】を $(b, j) = (1, 0), (1, 1), (0, 0)$ のそれぞれに対して計算し、 $s_{b,j}$ からなるベクトル $S(i) = (s_{1,1}, s_{1,0},$

$s_{0,0}$ )を出力する。また、このときの乱数発生器603の出力 $r_{b,j}$ は乱数保持器609に格納する。 $s(i)$ を記名付き交信手段605が安全チャネル105(i)を通じてセンタ100に送信する。センタ100は投票用紙受信手段626で受信した正当な有権者からの $s(i)$ を受信する。ブラインド署名生成器624は秘密保持手段621、定数保持手段622みだした $d_b$ 及び $n_b$ を用いて、

【0072】

【数9】

$$D_{b,j} = s_{b,j}^{d_b} \cdot \text{mod } n_b.$$

【0073】を各 $(b, j) = (1, 0), (1, 1), (0, 0)$ について計算し、出力する。ブラインド署名送信手段625は $D(i) = (s_{1,1}, s_{1,0}, s_{0,0})$ を投票者101(i)に送信する。

【0074】投票用紙作成を行なったすべての有権者に対して署名を送信すればセンタは投票フェーズに移行することを宣言する。以上が投票用紙設定フェーズである。

【0075】次に、投票フェーズを説明する。

【0076】署名検証手段606は、ブラインド署名受信手段611によりセンタ100から受信した $D(i)$ と、定数保持手段602から読み出した $e_b$ ,  $n_b$ を用いて

【0077】

【数10】

$$s_{b,j} = D_{b,j}^{e_b} \cdot \text{mod } n_b.$$

【0078】が各 $(b, j) = (1, 0), (1, 1), (0, 0)$ について成立するかどうか検証する。確認できれば、投票生成器607は、自分の意見 $B$  ( $B$ は0か1)に対して、乱数保持器609から読み出した整数 $r_{1,B}$ ,  $r_{0,0}$ と、定数保持手段602から読み出した $n_1$ ,  $n_0$ を用いて、

$$t_{1,B} = D_{1,B} / r_{1,B} \cdot \text{mod } n_1$$

$$t_{0,0} = D_{0,0} / r_{0,0} \cdot \text{mod } n_0$$

を計算し、無記名送信手段608は $T(i) = (t_{1,B}, t_{0,0})$ を送信者名を付記せずにセンタ100に送出する。

【0079】センタ100は、受信した $T(i)$ のうち $t_{0,0}$ を読み出し

【0080】

【数11】

$$\alpha = t_{0,0}^{e_0} \cdot \text{mod } n_0.$$

【0081】を計算する。 $\alpha$ は投票者が不正をしていなければ、 $v_{0,0}$ に等しくなる。 $\alpha$ を分割してRSA検証鍵 $e \cdot n$ を得、これと同じ検証鍵が以前使われているかどうかチェックする。使われていなければ、 $t_{1,B}$ の正当性を検証する。すなわち、

【0082】



## 【数12】

$$t_{1,B} \bmod n$$

【0083】が意見Bを表す正しいフォーマットに従った票であるかどうかを見、正しければこれを集計する。なお、同じ検証鍵が使われていれば、無効票として受理しない。

【0084】以上が投票フェーズである。全員の投票が\*

$$t_{1,B} = (d_{1,B} / r_{1,B} \bmod n_1) e_2 \bmod n_2$$

$$t_{0,0} = d_{0,0} / r_{0,0} \bmod n_0$$

として、投票文を暗号化すればよい。この場合  $n_1$  は  $n$  より小さいものとする。あるいは、第一の発明と第三の発明を両方実施する第5の実施例として、上記の第二\*

$$t_{1,B} = d_{1,B} / r_{1,B} \bmod n_1$$

$$t_{0,0} = (d_{0,0} / r_{0,0} \bmod n_0) e_2 \bmod n_2$$

と、投票タグを暗号化してもよい。この場合  $n_0$  は  $n_2$  より小さいものとする。

【0086】以下は上の実施例と同様なので説明を省略する。

【0087】また、第二の発明と第三の発明も同様にして同時に実現できる。

【0088】図5を参照すると、いづれの実施例で述べたシステムは、通信処理機能を備えたパーソナルコンピュータ等の端末装置 (TMU) 401と、読出し専用記憶装置 (ROM) 402と、ランダムアクセス記憶装置 (RAM) 403と、乱数発生器 (RNG) 404と、シグナルプロセッサ (SP) 406と、TMU401、ROM402、RAM403、RNG404およびSP406を相互に接続する共通バス405とから構成される。RNG404は乱数をSP406の指令により発生する。これはセンタ100が定数設定の時に用い、また、各投票者101(i)の乱数発生器として用いる。ROM407にはセンタ100の場合、定数  $e_i$ 、 $n_i$  ( $i=1, 0, 2$ ) と秘密情報  $d_i$  ( $i=1, 0, 2$ ) を記憶している。 $d_i$  ( $i=1, 0, 2$ ) はTUMからブラインド署名作成の度にRAMに格納するようにしてもよい。ROM407には投票者サブシステム101(i)の場合、定数  $e_i$ 、 $n_i$  ( $i=1, 0, 2$ ) を記憶している。ROM内に格納されたプログラムに基づいて、上述の動作を実現する。RAM403はこれらのステップの実行中に計算途中結果等を一時的に記憶するために用いられる。

【0089】また、システム100、101(i)は汎

\*終了したら、センタは結果公表フェーズへ移り、集計結果とすべての受理票およびタグ票を公開する。

【0085】次に、第一の発明と第三の発明を両方実施する第4の実施例について述べる。上記の第二の発明の実施例の投票文作成器607において、 $t_{1,B}$  を定数保持手段602から読み出した  $n_1$ 、 $n_2$ 、 $e_2$  を用いて、

10※の発明の実施例の投票文作成器607において、 $t_{1,B}$  を定数保持手段602から読み出した  $n_1$ 、 $n_2$ 、 $e_2$  を用いて、

用電子計算機等のデータ処理装置やICカードであってもよい。

【0090】本発明は選挙や投票以外にも、無記名電子アンケートや人気調査などに適用できる。

【0091】

20 【発明の効果】以上詳細に説明したように、本発明を用いれば、プライバシーを保ったまま異議申し立てができる無記名電子投票システムを実現することができる。

【図面の簡単な説明】

【図1】第一の発明の電子投票装置の一実施例を示すブロック図。

【図2】第一の発明の電子投票装置の一実施例を示すブロック図。

【図3】無記名電子投票システムを示す図。

【図4】準備フェーズの例を示す図。

30 【図5】センタ100、投票者サブシステム101(i)の構成を示す図。

【図6】第二の発明の電子投票装置の一実施例を示すブロック図。

【図7】第二の発明の電子投票装置の一実施例を示すブロック図。

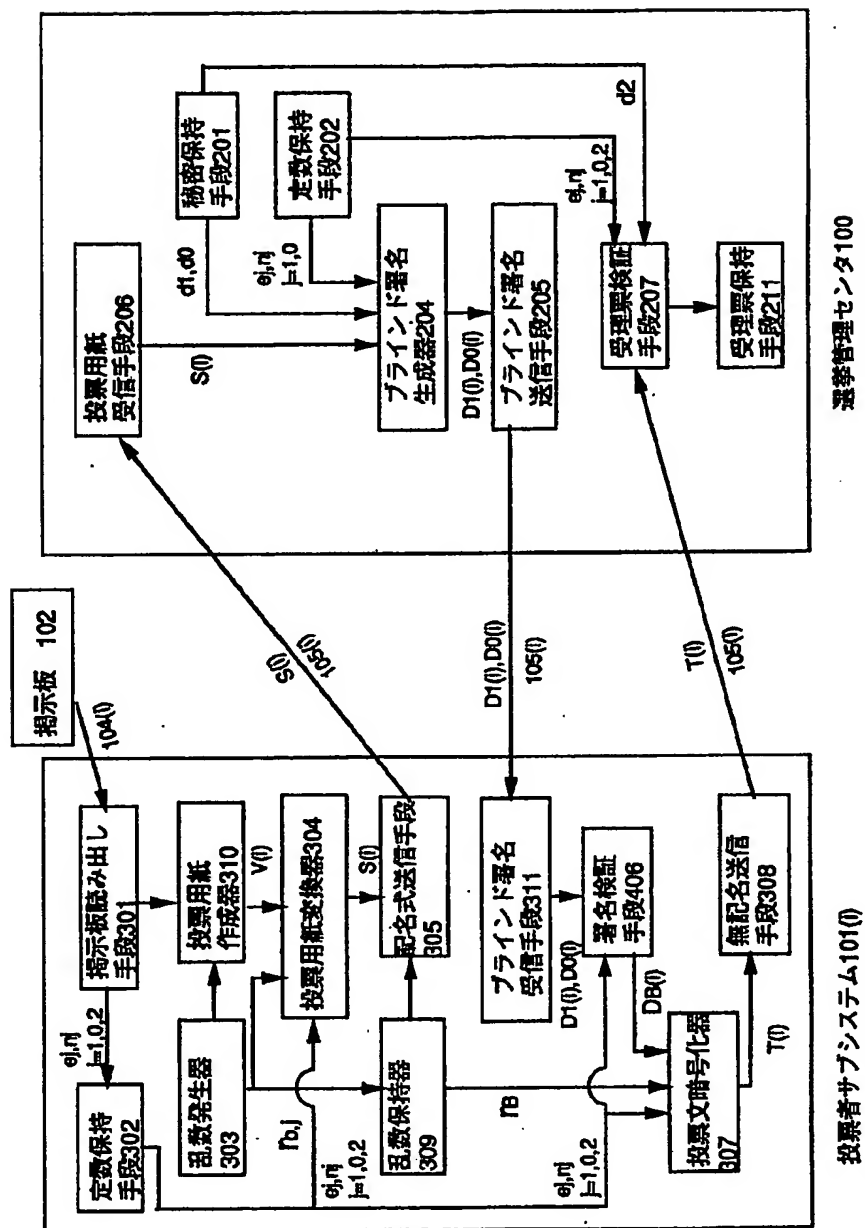
【図8】第三の発明の電子投票装置の一実施例を示すブロック図。

【符号の説明】

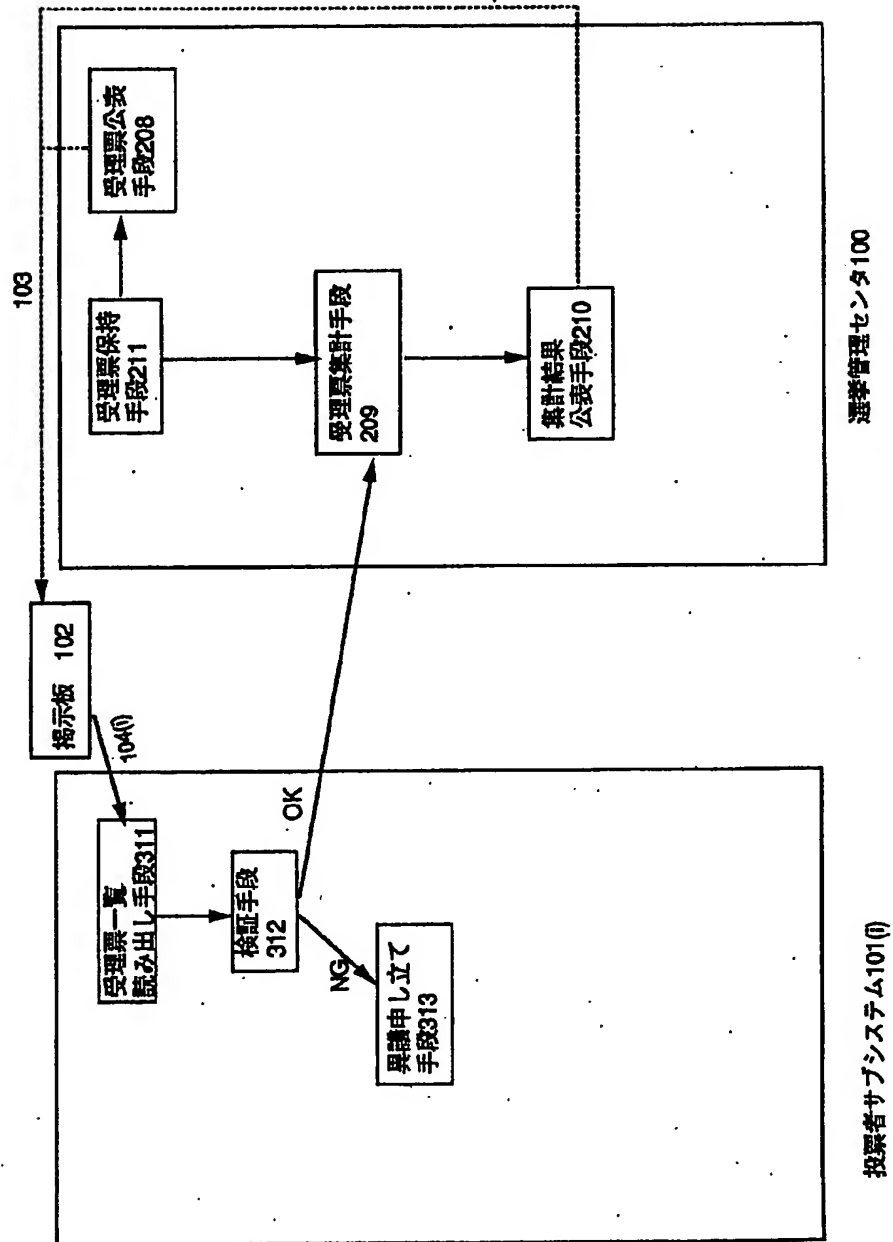
100 選挙管理センタ  
101(i) 投票者サブシステム  
102 電子掲示板



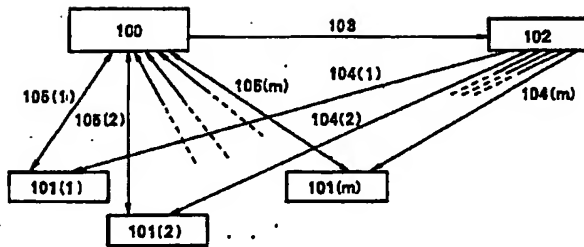
【図1】



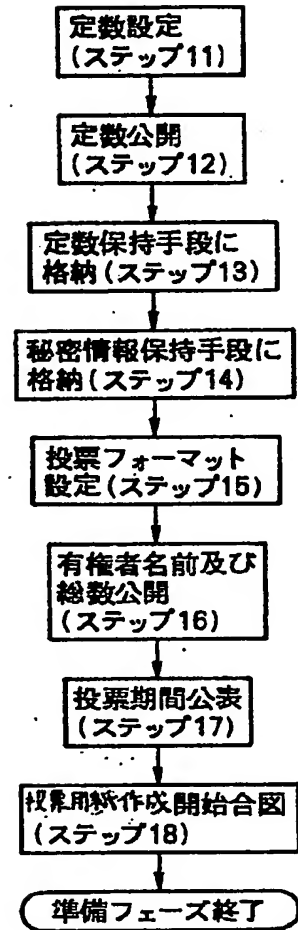
【図2】



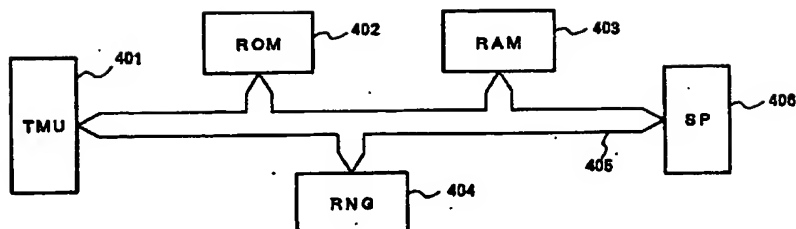
【図3】



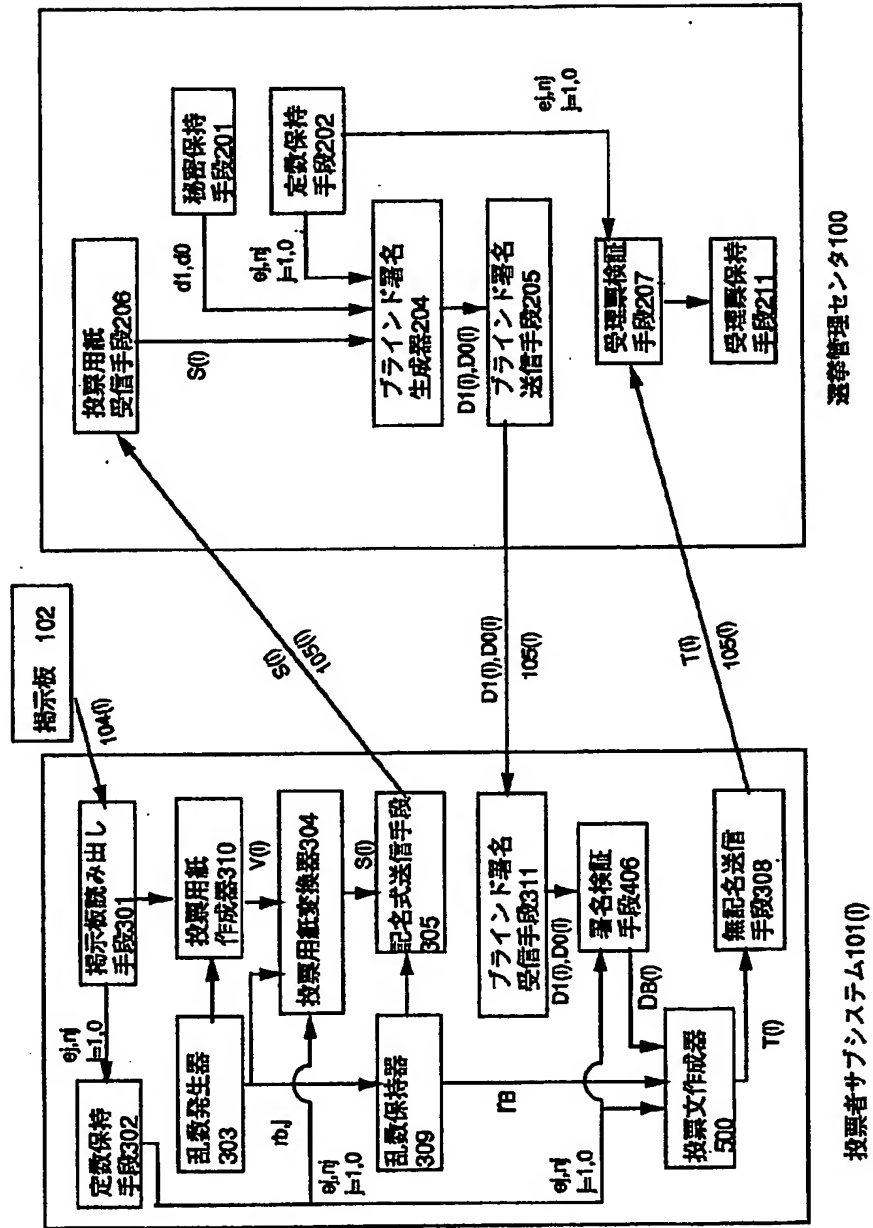
【図4】



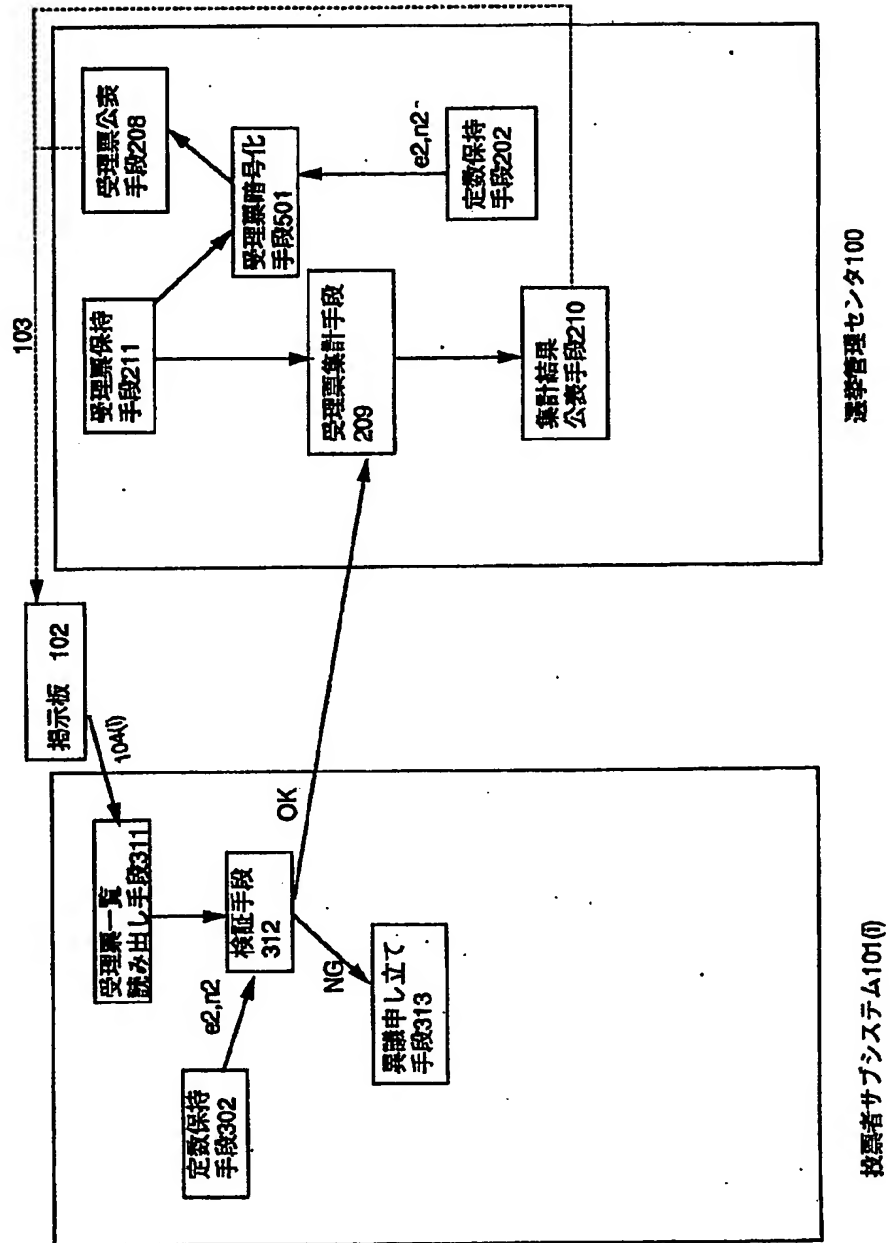
【図5】



【図6】



【図7】



【図8】

